REMARKS

In view of the following discussion and new arguments, the Applicants submit that none of the claims now pending in the application is unsupported under the provisions of 35 U.S.C. §112, directed to non-statutory subject matter under 35 U.S.C. §101, anticipated under the provisions of 35 U.S.C. §102, or obvious under the provisions of 35 U.S.C. §103. Thus, the Applicants believe that all of these claims are in allowable form.

I. REJECTION OF CLAIMS 10, 12, AND 13 UNDER 35 U.S.C. §101

Claims 10, 12, and 13 stand rejected as being allegedly directed to non-statutory subject matter. Specifically, the Examiner alleges that claims 10, 12, and 13 recite computer-readable media storing nonfunctional descriptive material that presents no functionality to satisfy the practical application requirement of 35 U.S.C. §101. The Applicants respectfully disagree.

MPEP 2106 states that in order for a claimed invention to accomplish a practical application under 35 U.S.C. §101, it must produce a "useful, concrete and tangible result." *State Street*, 149 F.3d at 1373-74, 47 USPQ2d at 1601-02. MPEP 2106 further goes on to say that a "useful" invention is one for which the utility is "(i) specific, (ii) substantial and (iii) credible". In this case, the Applicant submits that the utility of the claimed invention is specific (correlation of sensors in an intrusion detection system), substantial (aids in the identification of intrusions into a system), and credible (sharing of information detected by the sensors will improve performance).

A "concrete" result, according to MPEP 2106, is one that is "substantially repeatable". The adjustment of a first sensor's belief state, such that it is correlated to a second sensor's belief state, is repeatable and predictable.

A "tangible" result, according to MPEP 2106, is one that produces a "real-world result". As stated above, the result of the claimed invention is the adjustment of a first sensor's belief state, such that it is correlated to a second sensor's belief state. This adjustment is clearly an observable, "real-word" result.

Accordingly, because the invention recited in claims 10, 12, and 13 produces a useful, concrete, and tangible result, the Applicants respectfully submit that the claimed invention accomplishes a practical application, and, as such, cannot be directed to non-

statutory subject matter. Accordingly, the Applicants respectfully request that the rejection of claims 10, 12, and 13 under 35 U.S.C. §101 be withdrawn.

II. REJECTION OF CLAIMS 1-5 UNDER 35 U.S.C. § 112

Claims 1-5 stand rejected under 35 U.S.C. §112, first paragraph, for allegedly failing to comply with the written description requirement. Specifically, the Examiner alleges that the Specification fails to support the newly added limitations of resources that are "directly monitored" by the first or second sensor, belief states that relate to "apparent normal, degraded, or compromised state[s]" of monitored resources, and belief states that relate to "the existence or validity" of services supported on monitored resources. The Applicants respectfully disagree.

For instance, the Applicants submit that support for the limitation of resources that are "directly monitored" by sensors can be found at least at page A-3 of the Appendix (section entitled "Comprehending Multiple Sensors"), which is incorporated by reference, and which provides that the state of a sensor (*e.g.*, an eBayes-TCP sensor or an eBayes-Host sensor) is adjusted by updating a prior model of the sensor's world "based on the state of numerous features (directly observed or derived) linked to a set of unobservable hypotheses by conditional probability relationships" (emphasis added). Moreover, the Applicants submit that the phrase "directly monitored" is used in the normal English sense to mean that the resource or service is monitored by the sensor whose belief state is in question, and not by another sensor.

Support for the limitation of belief states that relate to "apparent normal, degraded, or compromised state[s]" of monitored resources and for the limitation of belief states that relate to "the existence or validity" of services supported on monitored resources can be found at least at page 5, second paragraph of the Applicants' Specification, where it is stated that, "[t]he belief state of the second sensor may indicate an apparent normal, degraded, or compromised state of a monitored system resource, the existence or validity of supported services, or any other relevant belief state held by a sensor in an intrusion detection system" (emphasis added).

As the Specification clearly supports the limitations in question, the Applicants submit that claims 1-5 comply with the written description requirement. Accordingly, the Applicants respectfully request that the rejection of claims 1-5 under 35 U.S.C. §112,

first paragraph be withdrawn.

III. REJECTION OF CLAIMS 1-2, 4-5, AND 10-13 UNDER 35 U.S.C. § 102

Claims 1-2, 4-5, and 10-13 stand rejected as being anticipated by the Purtell et al. patent (U.S. 6,950,947, issued September 27, 2005, hereinafter "Purtell"). The Applicants respectfully traverse the rejection.

Particularly, the Examiner's attention is directed to the fact that Purtell fails to disclose or suggest the novel method for correlating sensors in an intrusion detection system by adjusting a belief state of a first sensor regarding the state (normal/degraded/compromised), existence or validity of a system resource or service directly monitored by the first sensor, based on a belief state of a second sensor regarding the state, existence, or validity of system resource or service directly monitored by the second sensor, as claimed in Applicants' independent claims 1, 4, 5, and 10 - 13.

By contrast, Purtell discloses a set of peer firewalls/proxy servers that share information about transmission control protocol (TCP) control state in order to enhance the efficiency of TCP throughput in a network. Purtell says nothing about the need to monitor the network for suspected intrusions, *e.g.*, by using an intrusion detection system, as claimed by the Applicants in independent claims 1, 4, 5, and 10 - 13. A firewall, which filters data before it can reach the network (*See*, *e.g.*, column 1, lines 33-41 of Purtell), is not the same as an intrusion detection system, which identifies potential intrusions based on analysis of data that has already entered the network. That is, a firewall may be considered an intrusion prevention system, but not an intrusion detection system.

Moreover, even if the firewalls disclosed by Purtell could be considered to be equivalent to the intrusion detection sensors claimed by the Applicants, Purtell does not teach that the firewalls maintain or share "belief states" with respect to monitored resources. At best, the firewalls disclosed by Purtell simply share raw network state data in the form of common TCP control blocks (CCBs) that maintain the state of one or more TCP connections (*i.e.*, between a respective firewall and a given server). This data includes, for example, "round trip time (RTT) and variance, congestion controlled window size and threshold, local and remote maximum segment size (MSS),

retransmission and error rates, send and receive window rate, and maximum windows seen" (*See, e.g.*, column 4, lines 3-7 of Purtell). That is, the data that is exchanged is not analyzed to form a belief as to the state, existence, or validity of system resources or services, as claimed by the Applicants in independent claims 1, 4, 5, and 10 - 13.

In addition, even if the CCBs maintained by the firewalls of Purtell could be considered equivalent to a "belief state", the CCBs still fails to reflect the state of a monitored resource or service. Rather, the CCBs reflect the states of one or more TCP connections (*i.e.*, between a respective firewall and a given server, *See, e.g.*, column 4, lines 12-15 of Purtell).

Thus, Purtell fails to disclose or suggest the novel method for correlating sensors in an intrusion detection system by adjusting a belief state of a first sensor regarding the state (normal/degraded/compromised), existence or validity of a system resource or service directly monitored by the first sensor, based on a belief state of a second sensor regarding the state, existence, or validity of system resource or service directly monitored by the second sensor, as claimed in Applicants' independent claims 1, 4, 5, and 10 - 13. Specifically, Applicants' claims 1, 4, 5, and 10 - 13 positively recite:

1. A method for correlating a first sensor to a second sensor in an intrusion detection system, the first and second sensors each maintaining belief over a number of possible states of the system, the method comprising the steps of:

(a) transmitting to the first sensor information about the second sensor's belief state, said belief state indicating a state of at least one system resource or service directly monitored by the second sensor; and

(b) adjusting a prior belief state of the first sensor, said belief state indicating a state of at least one system resource or service directly monitored by the first sensor, the adjustment based at least in part on the second sensor's belief state. (Emphasis added)

4. A method for reducing false alarms generated by an intrusion detection system when a monitored resource is degraded or compromised, the intrusion detection system having a first and second sensors each maintaining belief over a number of possible states of the system, the method comprising the steps of:

(a) transmitting to the first sensor all or part of the belief of the second sensor regarding an apparent normal, degraded or compromised state of a resource directly monitored by the second sensor; and

(b) adjusting a prior belief state of the first sensor regarding an apparent normal, degraded or compromised state of a resource directly monitored by the first sensor so that an erroneous transaction with the degraded or compromised resource

does not generate an alarm. (Emphasis added)

5. A method for enhancing the sensitivity of an intrusion detection system that monitors a plurality of computer system resources, the intrusion detection system having a first and second sensors each maintaining belief over a number of possible states of the system, the method comprising the steps of:

(a) transmitting to the first sensor all or part of the belief of the second sensor regarding the existence or validity of services supported on computer system resources directly monitored by the second sensor; and

(b) adjusting a prior belief state of the first sensor regarding the existence or validity of services supported on computer system resources directly monitored by the first sensor so that an attempted communication with a nonexistent system service or resource appears suspicious. (Emphasis added)

10. A computer readable medium containing an executable program for correlating a first sensor to a second sensor in an intrusion detection system, the first and second sensors each maintaining belief over a number of possible states of the system, where the program performs the steps of:

(a) transmitting to the first sensor information about the second sensor's belief state, said belief state indicating a state of at least one system resource or service directly monitored by the second sensor; and

(b) adjusting a prior belief state of the first sensor, said belief state indicating a state of at least one system resource or service directly monitored by the first sensor, the adjustment based at least in part on the second sensor's belief state. (Emphasis added)

11. A computer readable medium containing an executable program for reducing false alarms generated by an intrusion detection system when a monitored resource is degraded or compromised, the intrusion detection system having a first and second sensors each maintaining belief over a number of possible states of the system, where the program performs the steps of:

(a) transmitting to the first sensor all or part of the belief of the second sensor regarding an apparent normal, degraded or compromised state of a resource directly monitored resource by the second sensor; and

(b) adjusting a prior belief state of the first sensor regarding an apparent normal, degraded or compromised state of a resource directly monitored by the first sensor so that an erroneous transaction with the degraded or compromised resource does not generate an alarm. (Emphasis added)

12. A computer readable medium containing an executable program for enhancing the sensitivity of an intrusion detection system that monitors a plurality of computer system resources, the intrusion detection system having a first and second sensors each maintaining belief over a number of possible states of the system, where the program performs the steps of:

(a) transmitting to the first sensor all or part of the belief of the second sensor

regarding the existence or validity of services supported on monitored computer system resources directly monitored by the second sensor; and

(b) adjusting a prior belief state of the first sensor regarding the existence or validity of services supported on computer system resources directly monitored by the first sensor so that an attempted communication with a nonexistent system service or resource appears suspicious. (Emphasis added)

13. A computer readable medium containing an executable program for enhancing the sensitivity of an intrusion detection system that monitors a plurality of computer system resources, the intrusion detection system having a first and second sensors each maintaining belief over a number of possible states of the system, where the program performs the steps of:

(a) transmitting to the first sensor all or part of the belief of the second sensor regarding the existence or validity of services supported on computer system resources directly monitored by the second sensor; and

(b) adjusting a prior belief state of the first sensor regarding the existence or validity of services supported on computer system resources directly monitored by the first sensor so that an attempted communication with a nonexistent system service or resource appears suspicious. (Emphasis added)

As discussed above, Purtell fails to disclose or suggest the novel method for correlating sensors in an intrusion detection system by adjusting a belief state of a first sensor regarding the state (normal/degraded/compromised), existence or validity of a system resource or service directly monitored by the first sensor, based on a belief state of a second sensor regarding the state, existence, or validity of system resource or service directly monitored by the second sensor, as claimed in Applicants' independent claims 1, 4, 5, and 10 - 13. Therefore, the Applicants submit that independent claims 1, 4, 5, and 10 - 13 fully satisfy the requirements of 35 U.S.C. §102 and are patentable thereunder.

Dependent claim 2 depends from claim 1 and recites additional features therefore. As such, and for at least the same reasons set forth above, the Applicants submit that claim 2 is not anticipated by the teachings of Purtell. Therefore, the Applicants submit that dependent claim 2 also fully satisfies the requirements of 35 U.S.C. §102 and is patentable thereunder.

IV. REJECTION OF CLAIM 3 UNDER 35 U.S.C. § 103

Claim 3 stands rejected as being unpatentable over Purtell in view of the Timm patent (U.S. 5,440,498, hereinafter "Timm"). The Applicants respectfully traverse the

rejection.

As discussed above, Purtell does not teach or even suggest the novel method for correlating sensors in an intrusion detection system by adjusting a belief state of a first sensor regarding the state (normal/degraded/compromised), existence or validity of a system resource or service directly monitored by the first sensor, based on a belief state of a second sensor regarding the state, existence, or validity of system resource or service directly monitored by the second sensor, as claimed in Applicants' independent claim 1, from which claim 3 depends. Applicants' claim 1 has been recited above. Timm does not bridge this gap in the teachings of Purtell. Purtell and Timm, singularly or in any permissible combination, thus fail to teach, suggest all of the limitations of Applicants' independent claim 1. Therefore, the Applicants submit that independent claim 1 fully satisfies the requirements of 35 U.S.C. §103 and is patentable thereunder.

Dependent claim 3 depends from claim 1 and recites additional features therefore. As such, and for at least the same reasons set forth above, the Applicants submit that claim 3 is not made obvious by the teachings of Purtell in view of Timm. Therefore, the Applicants submit that dependent claim 3 also fully satisfies the requirements of 35 U.S.C. §103 and is patentable thereunder.

V. CONCLUSION

Thus, the Applicants submit that all of the presented claims fully satisfy the requirements of 35 U.S.C. §112, 35 U.S.C. §101, 35 U.S.C. §102 and 35 U.S.C. §103. Consequently, the Applicants believe that all of these claims are presently in condition for allowance. Accordingly, both reconsideration of this application and its swift passage to issue are earnestly solicited.

If, however, the Examiner believes that there are any unresolved issues requiring the maintenance of the final action in any of the claims now pending in the application, it is requested that the Examiner telephone Mr. Kin-Wah Tong, Esq. at (732) 530-9404 so that appropriate arrangements can be made for resolving such issues as expeditiously as possible.

Respectfully submitted,

8/16/07
Date

Kin-Wah Tong, Attorney
Reg. No. 39,400
(732) 530-9404

Patterson & Sheridan, LLP
595 Shrewsbury Avenue
Shrewsbury, New Jersey 07702